PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-282672**
(43)Date of publication of application : **15.10.1999**

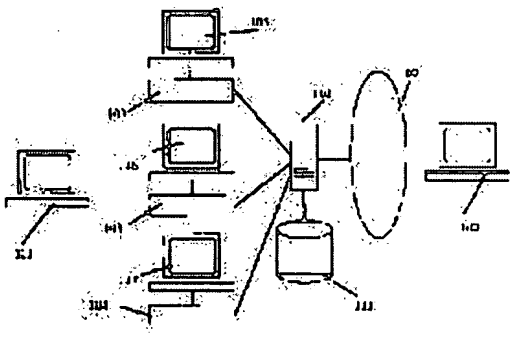
(51)Int.Cl. **G06F 9/06**

(21)Application number : **10-084836**
(22)Date of filing : **31.03.1998**

(71)Applicant : **HITACHI SOFTWARE ENG CO LTD**
(72)Inventor : **KONDO MARIKO**
TAGO SHIGERU

(54) TRANSFER METHOD AND EXECUTION SYSTEM FOR ON-LINE PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To directly prove that a program which is transferred on line has no dangerous operation by giving an electronic signature to the program when it's distributed via an inspector and confirming the signature to permit the execution of the transferred program before it's executed.
SOLUTION: A program producer produces programs via a program developing device 101, and the programs are copied and transferred to the program execution systems 105 to 107. The users (inspectors) of systems 105 to 107 execute the transferred programs to check whether the programs have dangerous operations. When it's confirmed that a function group to be inspected has no dangerous operation, the electronic signatures are given to the programs via the electronic signature devices 102 to 104. A program transmission request is given to a server system 110 from a program execution system 108 after the inspection, and the system 110 sends the data to the system 108.



LEGAL STATUS

[Date of request for examination]	23.06.2000
[Date of sending the examiner's decision of rejection]	12.08.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－282672

(43)公開日　平成11年(1999)10月15日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全 ８ 頁）

(21)出願番号　特願平10－84836

(22)出願日　平成10年(1998)３月31日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　近藤　麻里子
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　多胡　滋
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

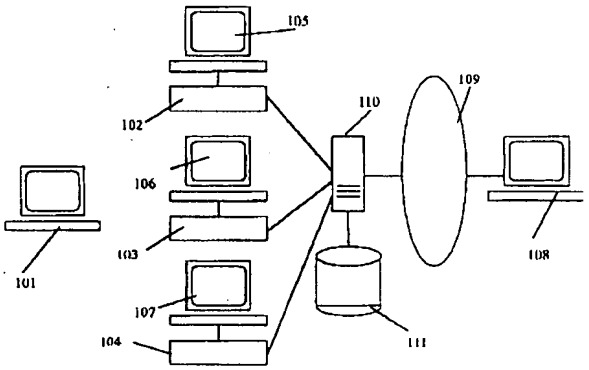
(54)【発明の名称】　オンラインプログラム転送方法およびオンラインプログラム実行システム

(57)【要約】

【課題】　プログラム開発者とは別に、そのプログラムが不正な動作をしないことをチェックし、電子署名を施す第３者（検証者）を用意することで、認証手続きを簡略化する。

【解決手段】　プログラムを計算機外部から計算機内部に転送するに先立ち、該プログラムの作成者以外の特定の人あるいは組織により、該プログラムを該プログラムの全体あるいは一部に、起動した人あるいは組織が認識不可能な動作をしないことを保証する電子署名を施し、該プログラムを起動する人あるいは組織による確認が行われた後に当該プログラムを計算機内部に転送する。

図１



1

【特許請求の範囲】

【請求項１】　オンラインで計算機内部に転送された後に起動されるプログラムの転送方法であって、
前記プログラムを計算機外部から計算機内部に転送するに先立ち、該プログラムの作成者以外の特定の人あるいは組織により、該プログラムを該プログラムの全体あるいは一部に、起動した人あるいは組織が認識不可能な動作をしないことを保証する電子署名を施し、該プログラムを起動する人あるいは組織による確認が行われた後に当該プログラムを計算機内部に転送することを特徴とするオンラインプログラム転送方法。

【請求項２】　前記電子署名を、前記プログラムの機能グループごとに異なる複数の人あるいは組織により施すことを特徴とする請求項１記載のオンラインプログラム転送方法。

【請求項３】　オンラインでプログラムを受信の後、該プログラムを演算処理装置上で実行するプログラム実行システムにおいて、
該プログラムの作成者以外の特定の人あるいは組織により、該プログラムの全体あるいは一部に電子署名が施されており、かつ該電子署名が確認された場合にのみ、該プログラムの実行を許可する手段を備えることを特徴とするオンラインプログラム実行システム。

【請求項４】　前記プログラムが有する機能グループのいずれに電子署名が施されているかを調べ、機能グループのいずれの実行を許可するかを変更する手段を備えることを特徴とする請求項３記載のオンラインプログラム実行システム。

【請求項５】　オンラインでプログラムを受信後、該プログラムを演算処理装置上で実行するプログラム実行システムにおいて、
複数の実行可能な機能の実行の許可あるいは不許可を、プログラム別および機能別に記憶する手段と、特定の機能を実行する直前に、該機能の実行の許可あるいは不許可を実行者に選択させる手段と、許可されている機能を実行させ、許可されていない機能を実行させない手段とを備えることを特徴とするオンラインプログラム実行システム。

【請求項６】　特定の機能を実行する直前に、該機能の詳細を実行者に示し、その機能の実行が実行者にとって不利益とならないことを実行者自身に確認させる手段を備えることを特徴とする請求項５記載のオンラインプログラム実行システム。

【請求項７】　複数の機能の許可あるいは不許可を、プログラム別および機能別に記録した設定データに対し、該設定データの作成者が電子署名を施す機能と、該設定データに対する該電子署名を確認する手段と、特定の設定データ作成者に対し、その作成者が作成した設定データの内容を取り込み、該プログラムの実行に当たって各機能の実行の許可あるいは不許可を該設定データに従って決定する手段を備え、あるプログラム実行システムにおいて設定された機能別の実行の許可あるいは不許可の設定を、その作成者による電子署名が確認された場合に、同一の、あるいは別のプログラム実行システムにおいて適用することを特徴とする請求項５または６記載のオンラインプログラム実行システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、オンラインでプログラムを受信の後、そのプログラムを実行する機能を備えた計算機などのオンラインプログラム実行システムおよびそのオンラインプログラムの転送方法に関するものである。

【０００２】

【従来の技術】ある計算機上でプログラムを実行する場合、そのプログラムを、予めその計算機に接続された補助記憶装置上に記憶しておき、実行時に読み出すことによって実行する方式が最も一般的であるが、一方で、プログラムはオンラインに接続されたサーバシステムの補助記憶装置上に記憶しておき、実行時に、オンライン経由でプログラムを計算機上に転送し、実行するという方法が多く利用されるようになっている。

【０００３】しかし、この方法では、利用者が該当するプログラムの実行開始を明示的に指示しない場合が多く、もしそのプログラムが利用者にとって不利益になるような動作をするものであったとしてもその動作を行う前に実行を中断する手段がない場合がある。

【０００４】このような危険を避けるため、該当するプログラムの全体あるいは一部に対して、そのプログラムの作成者が電子署名を施すことにより、利用者に対してプログラムが確かにその作成者によって作成されたものであり、他者によって改ざんされていないことを証明し、危険な動作をしないことを保証しようとする方法が主に用いられている。

【０００５】

【発明が解決しようとする課題】しかし、上述の従来の方法では、次のような問題がある。

【０００６】１）作成者が本人であることは証明できるが、そのプログラムが危険な動作をしないことを直接的には証明できない。危険な動作とは、利用者の許可なしに、ファイルのロックを解除する、ファイルを更新する、認証を与える、プログラムを更新するなど、利用者本人にとって不利益をもたらす動作、あるいはもたらすかも知れない動作のことである。従来は、作成者の組織名等を見て、信用する、しないを各利用者が適宜判断することで運用していた。

【０００７】２）多数のプログラムを実行させる場合、それらの作成者として多くの人あるいは組織を信用するようプログラム実行システムに設定する必要があり、作業が煩雑であり、また、信用度の検討が疎かになるとい

う弊害がある。

【０００８】３）危険な動作をするか、しないかの２者択一設定であるため、ある機能については危険な動作をしないプログラムであったとしても、別の機能について保証できなければ、そのプログラム全体を信用することができない。

【０００９】４）実行時のプログラム実行システムの環境や、プログラムに入力されるパラメータによって、実行者に不利益な結果を生む可能性がある。

【００１０】５）実行時のプログラム実行システムの環境や、プログラムに入力されるパラメータによって、実行者に不利益な結果を生む可能性がないにも関わらず、一般的に不利益な結果を生む可能性があるという理由で実行を許可されない場合がある。

【００１１】本発明の第１の目的は、このような問題を解決し、オンラインで転送されたプログラムが危険な動作をしないことを直接的に証明することができるオンラインプログラム転送方法およびオンラインプログラム実行システムを提供することにある。

【００１２】本発明の第２の目的は、実行者に不利益な結果を生じさせないようにすることができるオンラインプログラム実行システムを提供することにある。

【００１３】

【課題を解決するための手段】上記目的を達成するために、本発明のオンラインプログラム転送方法は、まず、プログラムの作成者とは別に、そのプログラムが危険な動作をしないことを検証できる人あるいは組織を用意する。プログラムの配布時に、この検証者によって電子署名を施す。利用者は、転送したプログラムを実行する前に電子署名を確認し、信用できる検証者によって電子署名されているプログラムであった場合は、その実行を許可する。

【００１４】さらに、そのプログラムの機能グループ別に検証者を用意し、その各々についての電子署名であることを明記した上で、プログラムに電子署名を施す。利用者は、自分が利用したい機能についてのみ、電子署名を確認し、その利用したい機能グループについて信用できる検証者によって電子署名されていた場合は、その機能グループの実行を許可する。

【００１５】また、上記第２の目的を達成するために、本発明のオンラインプログラム実行システムは、特定のプログラムをオンラインで受信後、実行する際に、複数の機能に対してその実行直前に、実行者に対して、その機能の実行を許可するかどうかを設定させる。

【００１６】さらに、各機能の実行の許可を設定する時点で、その機能の詳細を実行者に対して示すことにより、その機能の実行が実行者にとって不利益となるかどうかを実行者自身が判断できるようにする。

【００１７】そして、各機能に対する実行の許可／不許可の設定を記憶し、以降、同プログラムの実行時には同

機能を前期設定に基づいて実行あるいは不実行を決定する。

【００１８】また、記憶された各機能に対する実行の許可／不許可の設定データに対し、そのデータの作成者が電子署名を施し、そのデータの読み取り時に電子署名を確認する。

【００１９】

【発明の実施の形態】以下、本発明を図示する実施の形態を参照して詳細に説明する。

第１の実施形態

図１は、本発明の第１の実施形態のシステム構成図である。図１において、１０１は、本発明で対象としているプログラムを作成するためのプログラム開発装置である。１０２～１０４は、プログラムに対し電子署名を施す機能を持つ電子署名装置、１０５～１０８は、プログラムを演算処理装置内で実行する機能を持つプログラム実行システム、１０９はプログラムの転送に使用するオンラインシステムである。１１０は、オンライン経由でのプログラムの送信機能を持つサーバシステム、１１１はプログラムを記憶する機能をもつ補助記憶装置である。

【００２０】図２は、補助記憶装置１１１に記憶されるプログラムの構造を示している。図２において、２０１は、プログラム実行システム１０５～１０８上で実行可能なプログラム、２０２は、プログラム２０１に電子署名を施した人あるいは組織の名前、２０３は、プログラム２０１に電子署名を施した結果算出された電子署名データ、２０４は、前記の名前２０２によって危険な動作をしないことを保証された機能グループのＩＤ番号である。

【００２１】図３はプログラム実行システム１０８において、プログラム２０１を実行する前に設定するプログラム実行許可設定データの構造を示している。図３において、３０１は、プログラム２０１の機能グループのＩＤ番号、３０２は、機能グループ３０１が危険な動作をしないことを電子署名によって保証されているかどうかのフラグ（ＹＥＳまたはＮＯ）、３０３は、フラグ３０２に相当する電子署名を施した検証者の名前、３０４は、対応する機能グループの実行を許可するかどうかのフラグ（ＯＫまたはＮＯＴＯＫ）である。

【００２２】図４は、本実施形態の処理を示すフローチャートである。以下、図４に従い、本実施形態の詳細を説明する。最初に、プログラム２０１の作成者が、プログラム開発装置１０１上でプログラム２０１を作成する（ステップ４０１）。

【００２３】次に、プログラム２０１はコピーされて、プログラム実行システム１０５～１０７に転送される（ステップ４０２）。

【００２４】転送は、オンラインシステム１０９を使用しても使用しなくても良い。

5

【００２５】次に、実行システム１０５～１０７の使用者（検証者）によって、プログラム２０１が実行され、その動作が危険なものでないかどうかを検証する（ステップ４０３）。

【００２６】各検証は、各検証者ごとの機能グループに対して行われる。また、仕様書やソースプログラムコードの検証なども行われる。

【００２７】ステップ４０３の処理の結果、検証対象とした機能グループが危険な動作をしないこと確認された時点で、電子署名装置１０２～１０４によって電子署名が施される（ステップ４０４）。

【００２８】検証者の名前、ステップ４０４の電子署名の結果の電子署名データ、および検証した機能グループのＩＤがそれぞれ図２の２０２、２０３、２０４の欄に格納され、補助記憶装置１０１に記憶される（ステップ４０５）。

【００２９】検証の後、プログラム実行システム１０８からプログラム２０１の送信を要求されたサーバシステム１１０は、図２の２０１～２０４のデータをプログラム実行システム１０８に対して送信する（ステップ４０６）。

【００３０】プログラム実行システム１０８は、受信したデータを解析し、各電子署名データ２０３を確認し、図３に示したプログラム実行許可設定データを生成する（ステップ４０７）。

【００３１】生成されたデータに対し、利用者がフラグ３０４を格納する。このとき、利用者は、検証者の名前３０３を参照し、この機能グループが危険な動作をしないということを信用するかどうかを判断する（ステップ４０８）。信用する場合は、フラグ３０４として「ＯＫ」を設定し、電子署名があったとしても信用できない場合は、「ＮＯＴＯＫ」を設定する。

【００３２】次にプログラム２０１は、プログラム実行システム１０８上で、フラグ３０４が「ＯＫ」になっている機能グループのみを実行する（ステップ４０９）。

【００３３】このようにすることにより、１）プログラムの作成者とは独立した検証者によって検証済みであることが分かるので、そのプログラムが危険な動作をしないことを直接証明することができる。

【００３４】２）多数のプログラムに対して、共通の検証者が電子署名を施すことにより、電子署名の確認とプログラムの実行許可の設定作業を簡略化し、また、信用できる検証者かどうかの検討を充分行うことが可能となる。

【００３５】３）利用者が必要としている機能グループについてのみ、危険な動作をしないことが保証されるため、一部危険な動作をすることが保証されていない機能グループがあったとしても、その実行を許可することができる。

【００３６】第２の実施形態

6

図５は、本発明の第２の実施形態を示すシステム構成図である。

【００３７】図５において、５０１は、適当なプログラムを実行する機能を持つ演算処理装置、５０２は、文字や図表を表示する機能を持つディスプレイ装置、５０３は、設定データを保存するための補助記憶装置、５０４は、補助記憶装置５０３に保存されている設定データに対し、電子署名を施す機能を持つ電子署名装置、５０５は、プログラムの転送に使用するオンラインシステム、５０６はオンライン経由でのプログラムの送信機能を持つサーバシステム、５０７はプログラムを保存する機能を持つ補助記憶装置である。

【００３８】図６は、補助記憶装置５０３に保存されている設定データの構造を示している。

【００３９】図６において、６０１は、演算処理装置５０１によって実行可能な機能のＩＤ番号、６０２～６０４はＩＤ番号６０１の各機能に対し入力されるパラメータである。任意のパラメータに対する設定である場合は「＊」を格納する。６０５は、対応する機能６０１の実行を許可するか許可しないかを示すフラグである。

【００４０】図７は、機能別の実行許可／不許可の設定画面例を示す図である。図７において、７０１は機能の詳細を表示する枠、７０２～７０４はこの機能に対し入力されたパラメータである。各パラメータは適当な入力装置を介して変更することができる。７０５は、この機能の実行を許可するか許可しないかを入力するメニューである。

【００４１】図８は本実施形態の処理を示すフローチャートである。以下、図８に従い、本実施形態の詳細を説明する。まず、オンラインシステム５０５を介して、補助記憶装置５０７上に保存されているプログラムを、サーバシステム５０６から演算装置５０１に転送する（ステップ８０１）。次に、演算装置５０１上で、転送したプログラムを起動する。次に、補助記憶装置５０３に保存されている設定データが他者によって作成されたものである場合は、その電子署名を確認する（ステップ８０２、８０３）。そして、設定データの電子署名が正しいか、または自分自身が作成した設定データである場合は、それを演算処理装置５０１に読み出す（ステップ８０４）。

【００４２】次に、プログラムの各機能をその内容に従い順に実行してゆく（ステップ８０７）。起動中に実行する各機能について、設定データの機能ＩＤ番号６０１に登録されている機能かどうかをチェックする（ステップ８０８）。

【００４３】もし機能ＩＤ番号６０１に登録されており、かつ入力されたパラメータが６０２～６０４に登録されているものと一致しない場合は、図７に示した設定画面をディスプレイ装置５０２に表示する（ステップ８０９、８１０）。

7

【００４４】すなわち、図７の７０１には、実行しようとした機能の詳細を表示し、７０２～７０４には実行時に入力されたパラメータを表示する。

【００４５】実行者はこれらの情報を参照し、この機能の実行が不利益にならない場合は、メニュー７０５を「許可」に選択する（ステップ８１１、８１２）。

【００４６】一方、この機能の実行が不利益になる場合は、メニュー７０５を「不許可」に設定する（ステップ８１４）。

【００４７】この結果、図６の設定データの対応するＩＤ番号６０１の欄が追加され、入力されたパラメータと、「許可／不許可」のフラグが格納される（ステップ８１３、８１５）。

【００４８】ステップ８０９において、機能ＩＤ番号６０１および入力パラメータ６０２～６０４が一致した場合は、フラグ６０５に従ってその機能を実行するか、あるいは実行を中断する（ステップ８１７）。

【００４９】また、任意の時点で、電子署名装置５０４を使用して、補助記憶装置５０３上の設定データに対し電子署名を施し、この設定データを別のプログラム実行システムの補助記憶装置に複写することで、同一の設定ファイルを利用することができる。

【００５０】このようにすることにより、

１）各プログラムに対し、実行可能な機能と不可能な機能とを実行者自身が選択することにより、実行者に対し不利益とならない範囲で最大限の機能を実行することが可能となる。

【００５１】２）同一の実行環境にある複数のプログラム実行システムにおいて、実行の許可／不許可の設定を共有することにより、同一のプログラムを複数のプログラム実行システム上で効率よく実行することが可能となる。

【００５２】

【発明の効果】以上のように本発明によれば、オンラインでプログラムを受信後、そのプログラムを実行する機能を持つプログラム実行システムにおいて、次のような効果を得ることができる。

【００５３】１）プログラムの作成者とは独立した検証者が検証していることが分かるため、そのプログラムが危険な動作をしないことを直接的に証明することができる。

【００５４】２）多数のプログラムに対して、共通の検証者が電子署名を施すことにより、電子署名の確認とプログラムの実行許可の設定作業を簡略化し、また、信用できる検証者かどうかの検討を充分行うことが可能となる。

8

【００５５】３）利用者が必要としている機能グループについてのみ、危険な動作をしないことが保証されるため、一部危険な動作をすることが保証されていない機能グループがあったとしても、その実行を許可することができる。

【００５６】４）各プログラムに対し、実行可能な機能と不可能な機能とを実行者自身が選択することにより、実行者に対し不利益とならない範囲で最大限の機能を実行することが可能となる。

【００５７】５）同一の実行環境にある複数のプログラム実行システムにおいて、実行の許可／不許可の設定を共有することにより、同一のプログラムを複数のプログラム実行システム上で効率よく実行することが可能となる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態のシステム構成図である。

【図２】第１の実施形態におけるプログラムの構造を示す図である。

【図３】第１の実施形態におけるプログラムの機能グループの実行許可設定データの構造図である。

【図４】第１の実施形態における処理を示すフローチャートである。

【図５】本発明の第２の実施形態のシステム構成図である。

【図６】第２の実施形態における設定データの構造図である。

【図７】第２の実施形態における実行の許可／不許可の設定画面例を示す図である。

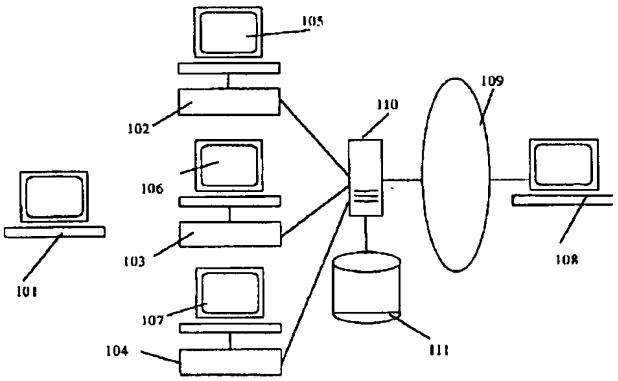
【図８】第２の実施形態における処理を示すフローチャートである。

【符号の説明】

１０１…プログラム開発装置、１０２～１０４…電子署名装置、１０５～１０８…プログラム実行システム、１０９…オンラインシステム、１１０…サーバシステム、１１１…補助記憶装置、５０１…演算処理装置、５０２…ディスプレイ装置、５０３…補助記憶装置、５０４…電子署名装置、５０５…オンラインシステム、５０６…サーバシステム、５０７…補助記憶装置。

【図１】

図１



【図２】

図２

201	202	203	204
プログラム	組織A	電子署名データA	F001
	組織B	電子署名データB	F002
	組織C	電子署名データC	F003

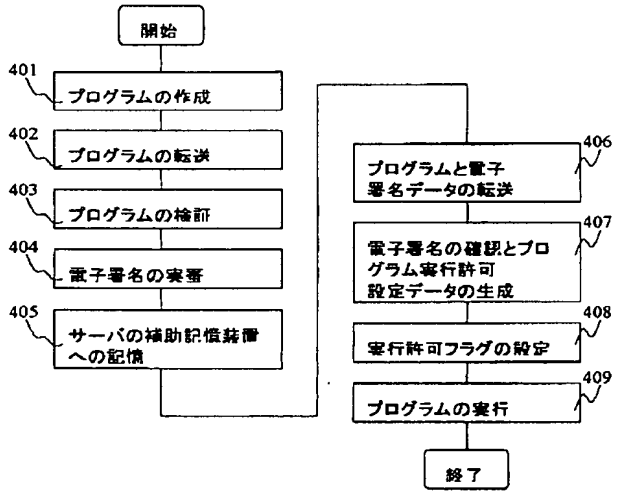
【図３】

図３

301	302	303	304
F001	YES	組織A	OK
F002	NO	組織B	NOTOK
F003	YES	組織C	OK

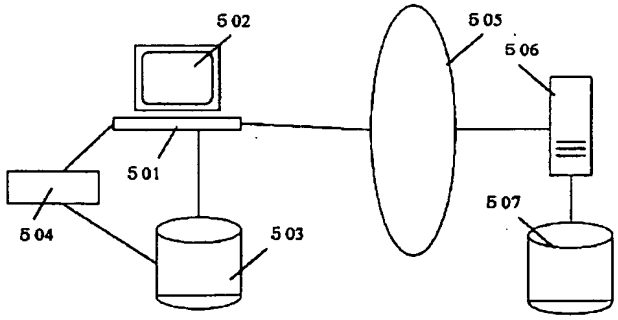
【図４】

図４



【図５】

図５



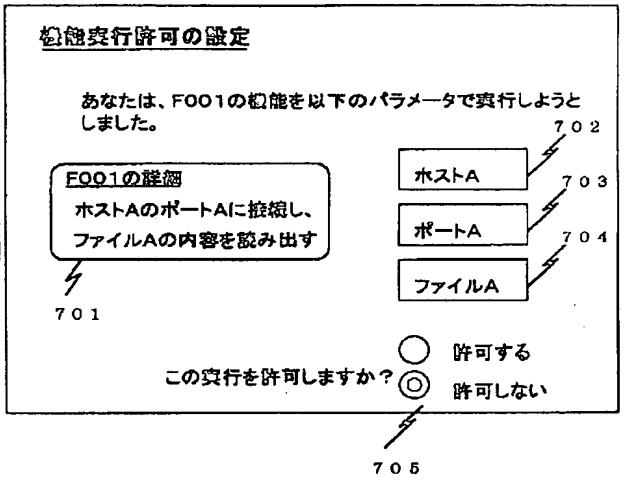
【図６】

図６

601	602	603	604	605
F001	ホストA	ポートA	ファイルA	OK
F001	ホストA	ポートB	ファイルB	OK
F001	ホストA	ポートC	*	NOTOK
F002	ファイルC	1024	"String"	OK
F003	ホストA	*	*	NOTOK
F003	ホストA	ファイルB	*	NOTOK
F003	ホストA	ファイルB	等N行	OK

【図７】

図７



【図８】

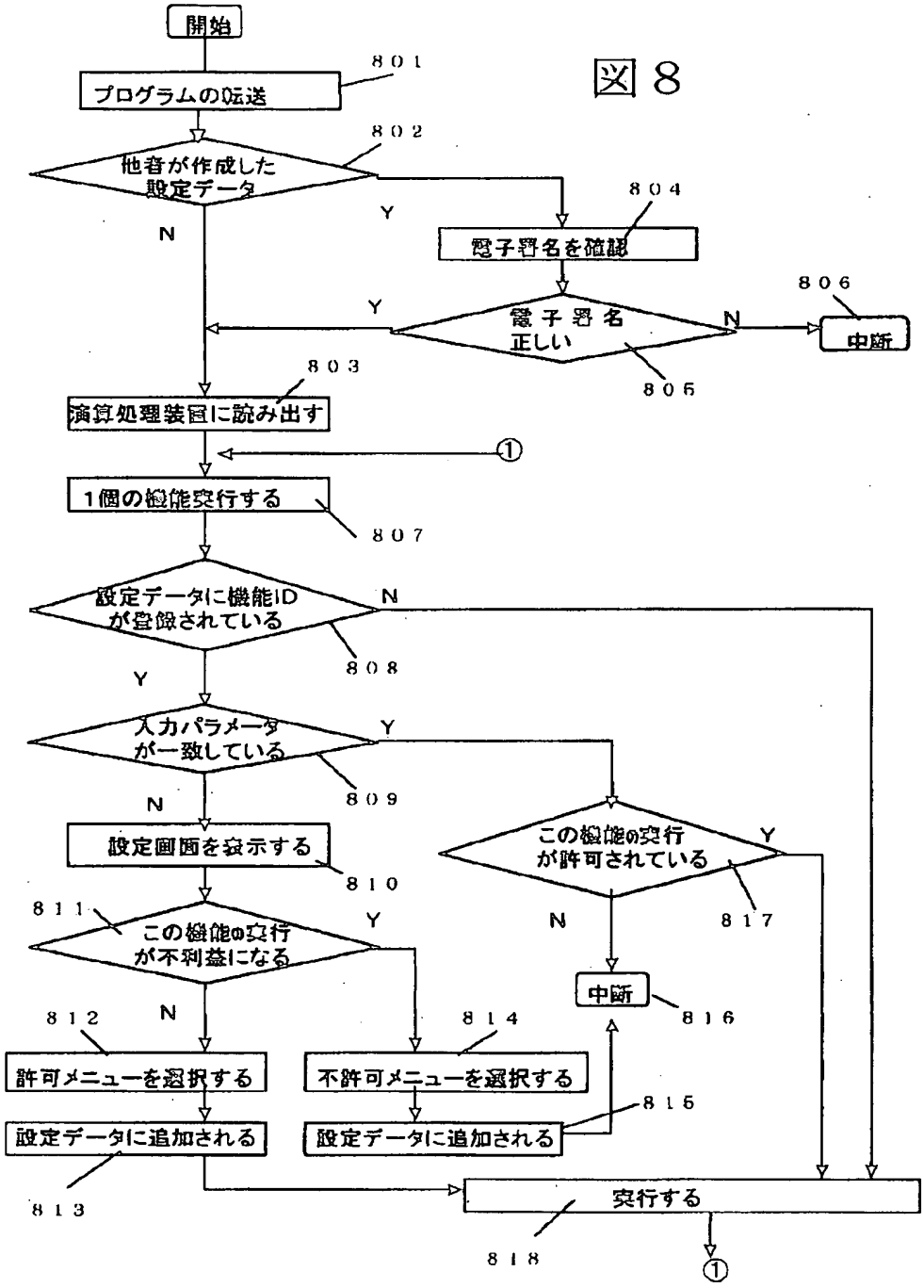

開始
801
プログラムの転送
802
他者が作成した設定データ
Y
N
804
電子署名を確認
806
Y
電子署名正しい
N
中断
805
803
演算処理装置に読み出す
①
1個の機能実行する
807
設定データに機能IDが登録されている
N
808
Y
入力パラメータが一致している
Y
809
N
設定画面を表示する
810
この機能の実行が許可されている
Y
817
N
811
この機能の実行が不利益になる
Y
中断
816
812
N
814
許可メニューを選択する
不許可メニューを選択する
815
設定データに追加される
設定データに追加される
813
実行する
818
①

図８